

Privacy Policy for Restaurant POS

Last updated: March 7, 2026

Restaurant POS is an offline restaurant POS app for Android that supports table ordering, kitchen order tickets (KOT), bar confirmation workflows, billing, credit ledger, stock management, staff management, reporting, and local network (LAN) synchronization between authorized business devices.

This Privacy Policy explains how Restaurant POS accesses, stores, processes, uses, and in limited cases shares information when the app is used. It is intended for business operators, staff users, and, where relevant, restaurant customers whose information is entered into the app during restaurant operations.

Important summary for the current March 2026 release:

- Core restaurant operational data is stored on the business's local devices
- Operational data is synchronized only between authorized devices on the same business LAN
- We do not operate a developer-hosted cloud database for routine restaurant operational data in this release
- Encrypted backups are created locally by the user
- External data flows may still occur in limited cases, such as user-initiated sharing, ads if enabled, or future integrations enabled in later releases

1. Who We Are

Restaurant POS is a restaurant point-of-sale and operations app published on Google Play.

Publisher/Developer: MetaNest

Privacy contact:metanest.app@outlook.com

If you are a restaurant guest or customer and your information was entered into the app by a restaurant, cafe, bar, or similar business, that business is generally responsible for deciding what customer data is entered into the app and how long it is retained. In that case, your first privacy contact should usually be the business using the app.

2. Scope

This Privacy Policy applies to the Restaurant POS Android app, including its offline-first restaurant POS features, local storage, LAN synchronization, reporting, backups, optional ad display, and optional integrations that may be enabled in certain releases. This Privacy Policy does not apply to third-party apps, websites, or services that users open from the app,

including WhatsApp, SMS apps, printers, Google Play services, Google AdMob, or other third-party platforms subject to their own terms and privacy policies.

3. Information the App Handles

Depending on how the app is configured and used, Restaurant POS may access, store, process, or in limited cases transmit the following categories of data:

In this Privacy Policy, words such as "collect", "process", "handle", or "use" include data that is:

- entered into the app by the business or its staff
- stored locally on a device running the app
- synchronized to other authorized devices on the same LAN
- shared to a third-party service because the user chose a sharing action or because an enabled third-party SDK or integration is active

These words do not mean that all restaurant operational data is uploaded to the developer's own remote servers.

A. Business and venue information

- Restaurant or venue name
- Logo or branding reference
- Business address
- Business phone number
- Support email
- GSTIN, FSSAI number, UPI ID, WhatsApp number
- Billing and invoice settings

B. Staff and account information

- Admin and staff names
- Staff phone numbers, where entered
- Role and permission settings
- Encrypted or hashed authentication information such as PIN hashes
- Staff session timestamps and limited device/session information

C. Restaurant operations data

- Table numbers, areas, seat labels, and table status
- Menu categories, menu items, item codes, barcodes, tax settings, and item images
- Orders, order items, item notes, KOT records, bar confirmations, and service status
- Checkout and billing records
- Payment mode details such as cash, UPI, card, credit, split payment details, UTR/reference entries, and optional card last-4 references if entered by the operator
- Customer name, phone number, address, and delivery details where entered
- Credit ledger entries and repayment records

- Stock items, stock movement records, and stock-link mappings
- Audit logs and business reports

D. Local network and device data

- Local network host or IP information needed to connect business devices on the same LAN
- Configured server port and connection state
- Limited operational diagnostics required for local synchronization, LAN security, or transport troubleshooting

E. Camera and barcode-scanning data

- Camera access is used only when a user chooses barcode-scanning features
- Barcode content scanned through the camera or scanner input
- For the barcode-scanning feature used in the current app build, scanning is processed on-device

F. Exported and shared business files

- PDF bills created by the app
- CSV or PDF reports exported by the app
- Encrypted local backup files created by the app

G. Advertising data

If in-app ads are enabled in a free-tier configuration, the Google Mobile Ads SDK (AdMob) may automatically collect and share data such as:

- IP address
- User product interactions
- Diagnostic information
- Device and account identifiers, including advertising-related identifiers where available

These data practices are controlled in part by Google and are described further in Google's documentation and privacy terms.

H. Optional subscription and purchase data

The March 2026 release of the app has subscription upgrade runtime disabled. If subscriptions or plan purchases are enabled in a future release, the app may process:

- Product identifiers
- Purchase tokens
- Order identifiers
- Package name
- License verification data
- Device integrity attestation data where configured

Such processing would be used only for purchase verification, subscription management, fraud prevention, and entitlement enforcement.

4. How Information Is Handled

The app handles information in the following ways:

- Information entered by an admin, cashier, waiter, bar manager, kitchen user, or other authorized business user
- Information generated during restaurant operations, such as orders, KOT updates, bills, stock changes, and audit events
- Information synchronized between authorized devices on the same business LAN
- Information created when a user exports a report, shares a bill, or creates an encrypted local backup
- Information automatically collected by integrated third-party SDKs, such as AdMob, when those SDKs are active

We do not operate a general cloud database for day-to-day restaurant operations in the current app release. Core operational data is primarily stored and processed locally and, where needed for multi-device operation, synchronized over the business's local network.

5. How We Use Information

We use information to:

- Provide and operate restaurant POS functionality
- Authenticate authorized users and manage role-based access
- Create and manage tables, orders, KOTs, bar confirmations, bills, payments, and stock
- Generate reports, exports, and local encrypted backups
- Synchronize data between authorized business devices on the same LAN
- Protect the app, detect misuse, investigate failures, and maintain security
- Comply with legal, accounting, tax, audit, and recordkeeping obligations
- Display ads in supported free-tier configurations
- Verify plan purchases or subscriptions if those features are enabled in a future release

6. Legal Bases for Processing

Where required by applicable law, we rely on one or more of the following legal bases:

- Performance of a contract or steps requested before entering into a contract
- Legitimate interests in operating, securing, improving, and supporting the app and related business workflows
- Compliance with legal obligations, including tax, accounting, fraud prevention, and recordkeeping obligations
- Consent, where required for specific processing activities such as certain advertising or device-permission flows

If you are a restaurant customer whose information is entered by a business using Restaurant POS, that business may rely on its own legal bases under local law for customer order, billing, tax, or delivery processing.

7. How Information Is Shared

We do not sell personal information.

We may share or make information available in the following limited circumstances:

A. Authorized business devices on the same local network

Operational data may be synchronized between authorized devices used by the same business, such as admin, waiter, kitchen, bar, cashier, or other approved role-based devices connected over the same LAN.

B. User-initiated sharing

When a user chooses to share a bill or document, the app may pass the selected content to third-party apps or services chosen by the user, such as:

- WhatsApp
- SMS apps
- Print services
- PDF viewers or file-sharing targets

C. Third-party service providers and platforms

Depending on build configuration and usage, the app may interact with:

- Google Play services
- Google AdMob / Google Mobile Ads SDK
- Google Play Billing
- Google Play Integrity

These services process data under their own privacy terms and policies.

D. Legal and safety reasons

We may disclose information if required to do so by law, regulation, court order, valid legal request, or where reasonably necessary to protect rights, security, property, users, or the public.

8. Local Storage, LAN Sync, and Data Location

Restaurant POS is designed as an offline-first restaurant POS app.

- Core operational data is stored primarily in the app's local database

- In many deployments, the admin device acts as the business's authority device
- Authorized staff devices may receive synchronized copies of operational data needed for their role
- Routine restaurant operations do not require a central developer-hosted cloud database in the current release

Because the app supports LAN synchronization, copies of relevant operational data may exist on multiple authorized business devices, not only on the admin device.

For clarity:

- In the current app build, routine restaurant operational data is not intended to be sent to a developer-managed cloud backend
- Local encrypted backups are created on-device by the business user
- Google Drive backup is not configured in the current build unless a future provider is added
- If in-app ads are enabled, the ad SDK may send limited device or usage data to Google
- If a user chooses to share a bill or report through WhatsApp, SMS, print, or another app, that selected content is shared by the user's action

9. Security Measures

We use reasonable technical and organizational measures designed to protect information processed by the app. These measures include, where applicable:

- PIN hashing for authentication data
- Encryption of sensitive settings at rest using Android Keystore-backed encryption
- Encrypted local backup files
- App-level restrictions on platform backup and device-transfer backup
- Role-based access controls
- Audit logging for important business actions
- LAN transport restrictions intended for local/private network use
- Certificate pinning and integrity checks for enabled monetization verification features
- Secure file sharing through Android `FileProvider` where applicable

No method of storage, transmission, or security control is completely foolproof, and we cannot guarantee absolute security.

10. Data Retention

We retain information for as long as necessary for the purposes described in this Privacy Policy, unless a longer retention period is required or permitted by law.

In practice:

- Operational restaurant data is usually retained locally until the business deletes it, overwrites it, uninstalls the app, restores from another backup, or otherwise removes it through app or device controls

- Audit, billing, tax, credit, and compliance records may be retained longer where needed for legitimate business, security, or legal reasons
- Exported files and backups remain where the business stores them unless deleted
- Third-party services such as AdMob or Google Play may retain data under their own policies

Where account deletion or data deletion is requested, we may retain limited information where necessary for fraud prevention, security, dispute resolution, tax, accounting, or legal compliance.

11. Your Rights and Choices

Depending on where you live, you may have rights such as:

- Access to personal information
- Correction of inaccurate information
- Deletion of personal information
- Restriction or objection to certain processing
- Data portability, where applicable
- Withdrawal of consent where processing is based on consent
- Lodging a complaint with a data protection authority or regulator

For business operators and staff

If you are the business using Restaurant POS, you can generally review and manage much of your business data through the app's administrative functions, exports, backups, and account-management controls.

For restaurant customers

If your name, phone number, address, order, credit, or billing information was entered into Restaurant POS by a restaurant, bar, cafe, or similar business, please contact that business first to exercise your privacy rights. That business is typically the primary controller of customer transaction data entered into the app during service.

Advertising choices

If ads are shown, certain ad-related identifiers may be controlled through your Android device settings. You may also review Google's advertising and privacy controls for additional options.

12. Children's Privacy

Restaurant POS is a business application intended for restaurant and hospitality operations. It is not directed to children and is not intended for use by children as a consumer app.

We do not knowingly collect personal information directly from children through the app as an independent consumer service. If you believe that personal information relating to a child

has been entered into the app inappropriately, please contact the relevant business operator and/or us using the contact details below.

13. International Use and Transfers

Restaurant POS may be used in multiple countries. Core restaurant operational data is designed to remain local to business devices in the current release. However, if third-party services such as Google AdMob, Google Play Billing, Google Play Integrity, messaging apps, or similar platforms are used, those providers may process data in other countries in accordance with their own privacy terms and applicable law.

14. Third-Party Services and Links

Relevant third-party privacy resources may include:

- Google Play User Data policy:
<https://support.google.com/googleplay/android-developer/answer/10144311>
- Google AdMob data disclosure:
<https://developers.google.com/admob/android/privacy/play-data-disclosure>
- Google Privacy Policy: <https://policies.google.com/privacy>
- Google Ads technologies: <https://policies.google.com/technologies/ads>
- ML Kit: <https://developers.google.com/ml-kit>

We are not responsible for the privacy practices of third-party services outside our control.

15. Changes to This Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in the app, legal requirements, business practices, or third-party integrations. If we make changes, we will update the "Last updated" date above. Material changes may also be communicated through the app, website, release notes, or Google Play listing where appropriate.

16. Contact Us

If you have questions, requests, or complaints about this Privacy Policy or data handling related to Restaurant POS, contact:

Publisher/Developer: MetaNest
Privacy contact: metanest.app@outlook.com